IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO

United States of America,	**Case No. 1:24CV2061**
Plaintiff,	
-vs-	**JUDGE PAMELA A. BARKER**
947,883 Tether ("USDT") Cryptocurrency valued at approximately $947,883.00, formerly associated with Cryptocurrency address beginning/ending 0x7d5…48a8306,	**FINAL ORDER OF FORFEITURE**
Defendant.	

Pursuant to 18 U.S.C. § 981(a)(1)(C) (proceeds of wire fraud/conspiracy to commit wire fraud) and 18 U.S.C. § 981(a)(1)(A) (money laundering), this is an action for the civil forfeiture of the Defendant 947,883 Tether ("USDT") Cryptocurrency valued at approximately $947,883.00, formerly associated with Cryptocurrency address beginning/ending 0x7d5…48a8306 (hereinafter "Defendant Property"). Currently pending is the United States of America's Motion for a Final Order of Forfeiture with respect to the Defendant Property. (Doc. No. 6.) The docket reflects that no claims and/or answers to the Complaint were filed, and no opposition was filed to the instant Motion.

For the following reasons, the United States' Motion (Doc. No. 6) is GRANTED.

I. Relevant Background

A. Factual Allegations

On November 26, 2024, the United States filed a verified Complaint in Forfeiture against the Defendant Property. (Doc. No. 1.) Therein, the United States alleges, in relevant part, as follows.

The FBI Cleveland Field Office is investigating cryptocurrency confidence fraud scams, perpetrated on victims throughout the United States, including in the Northern District of Ohio. (*Id.* at ¶ 29.) These schemes often begin in a number of ways, such as a misdialed text to WhatsApp message or making a connection online with a new person via a social media or dating website. (*Id.* at ¶ 30.) From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics expressing care and concern for the victim before making escalating requests for money, often via cryptocurrency. (*Id.*)

On or about October 20, 2023, a victim in Elyria, Ohio, with the initials "J.S." filed a complaint with the FBI's Internet Crime Complaint Center reporting losses from a computer tech scam. (*Id.* at ¶ 31.) The incident began when J.S. noticed an alert on his MacBook laptop screen telling him his computer was compromised and telling him to call a telephone number to resolve the issue. (*Id.* at ¶ 32.) An individual using the suspected alias "Allan Walton" ("Walton") answered the telephone stating that he was an Apple employee, and falsely stating that J.S.' s retirement account at his financial institution ("financial institution-1") had been compromised. (*Id.*)

While on the telephone with J.S., Walton added an individual using the suspected alias "Stephen Gruber" ("Gruber"), who claimed to be the senior risk and fraud analyst employee on the case regarding J.S.'s computer. (*Id.* at ¶ 33.) Gruber falsely told J.S. that three separate transactions - in the amounts of $23,152.00, $31,421.67, and $36,278.71 - had taken place moving money from J.S.'s account at financial institution-1. (*Id.* at ¶ 34.) Gruber told J.S. that the recipients of the claimed transfers were in either China or Russia, in addition to one going directly to a casino in Las Vegas. (*Id.*) Gruber advised J.S. that the transaction sent to the casino could potentially be stopped with the

assistance of the Federal Trade Commission. (*Id*.) Gruber told J.S. that to keep his money safe, J.S. would need to wire money at the direction of Gruber and/or Walton. (*Id*.)

Walton instructed J.S. to download a screen sharing service onto his MacBook. (*Id*. at ¶ 35.) This gave Walton access to J.S.'s computer. (*Id*.) Using this access, Walton created an account at a virtual currency exchange (VCE-1) using an email account associated with J.S. (*Id*.) On two separate occasions, Walton then directed J.S. to wire funds to the newly created account at VCE-1 from J.S.'s personal bank account at another financial institution ("financial institution-2"). (*Id*. at ¶ 36.) On October 18, 2023, J.S. wired $145,000.00 into the newly created account at VCE-1 via his personal account at financial institution-2. (*Id*. at ¶ 37.) On or about October 19, 2023, a confirmation email was sent to s******j***465@gmail.com from VCE-1 confirming the deposit of $145,000.00 credited to J.S.'s cryptocurrency wallet held at VCE-1; address beginning/ending: 0x4FA . . . e991a3d (ADDRESS-1). (*Id*.) On October 19, 2023, using his control of J.S.'s MacBook via the screen sharing software, Walton withdrew approximately 84.98 Ethereum ($133,749.00) from J.S.'s account at VCE-1. (*Id*. at ¶ 38.) Publicly available websites confirm this transaction took place on the Ethereum blockchain.[1] (*Id*.)

The following day, on October 20, 2023, at the direction of Gruber and/or Walton, J.S. wired another $115,000.00 into the newly created account at VCE-1 via his personal account at financial institution-2. (*Id*. at ¶ 39.) That same day, a confirmation email was sent to s******j***465@gmail.com from VCE-1, confirming the deposit of $115,000.00 credited to J.S.'s cryptocurrency wallet held at ADDRESS-1. (*Id*.) On October 23, 2023, using his control of J.S.'s

[1] The specific blockchain transaction hash for this transaction (as well as the blockchain transactions discussed *infra*) are set forth in the verified Complaint and will not be repeated herein.

MacBook via the screen sharing software, Walton withdrew approximately 75 Ethereum ($120,000.00) from J.S.'s account at VCE-1. (*Id*. at ¶ 40.) Publicly available websites confirm this transaction took place on the Ethereum blockchain. (*Id*.)

On November 1, 2023, at the direction of Gruber and/or Walton, J.S. wired approximately $165,000.00 to a different virtual currency exchange (VCE-2) from J.S.'s personal account at financial institution-2, where it was converted to Tether (USDT). (*Id*. at ¶ 41.) On November 2, 2023, using his control of J.S.'s MacBook via the screen sharing software, Walton took approximately $155,093.00 worth of the $165,000.00 that was converted to USDT at VCE-2 and transferred it to ADDRESS-1. (*Id*. at ¶ 42.) On November 2, 2023, using his control of J.S.'s MacBook via the screen sharing software, Walton withdrew approximately 155,093 USDT ($155,093.00) from ADDRESS-1. (*Id*. at ¶ 43.) Publicly available websites confirm that both of these transactions took place on the Ethereum blockchain. (*Id*. at ¶¶ 42, 43.)

After the transactions to ADDRESS-1 were completed, J.S. called financial institution-1 to ask about the wires Walton claimed were sent to China, Russia, and the casino in Las Vegas. (*Id*. at ¶ 44.) The employee at financial institution-1 advised J.S. that the transactions never occurred. (*Id*.) As a result of the cryptocurrency fraud scam, J.S. (a senior citizen) lost a total of approximately $425,000-- his entire life savings. (*Id*. at ¶ 45.) J.S. and his wife are currently living off Social Security and assistance from a relative. (*Id*.)

After receiving J.S.'s complaint, the FBI conducted an investigation, including a tracing analysis using the First In First Out ("FIFO") accounting methodology. (*Id*. at ¶ 48.) The details of the FBI's tracing analysis are set forth in great detail in the Complaint in Forfeiture and will not be repeated herein. (*Id*. at ¶ 48.) In sum, approximately $415,093.00 of J.S.'s funds were

wired/transferred to J.S.'s cryptocurrency wallet held at ADDRESS-1. (*Id*.) Using the access and control he had of J.S.'s computer - Walton withdrew 84.98 Ethereum ($133,749.00) from ADDRESS-1 on or about October 19, 2023. (*Id*.) Thereafter, the fraudsters "swapped" this cryptocurrency [namely, 84.98 Ethereum ($133,749.00) withdrawn from ADDRESS-1] from one type of cryptocurrency to another and engaged in several transfers from one cryptocurrency address to another, which served the purpose of commingling J.S.'s funds with other funds. (*Id*.) *See also* Doc. No. 1 at ¶¶ 47, 49, 52, 53.

Of the 84.98 Ethereum ($133,749.00) withdrawn by Walton from ADDRESS-1, the FBI was able to trace - through several steps of "blockchain analysis"[2] and using the FIFO accounting methodology - approximately $105,615.00 of J.S.'s funds to the subject cryptocurrency address beginning/ending 0x7d5 . . . 48a8306 ("the subject cryptocurrency address"). (*Id.* at ¶ 47.) Particularly, the final step of the FBI's blockchain analysis showed that on or about December 14, 2023, a total of approximately 355,077 USDT was transferred from another cryptocurrency address to the subject cryptocurrency address, including the $105,615.00 (now 105,615 USDT) that originated in J.S.'s account.[3] (*Id*. at ¶ 48(R).) At the time of the transfer, the subject cryptocurrency

---

[2] Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. (*Id*. at ¶ 25.)

[3] Tether (USDT) is a "stablecoin," a type of blockchain -based currency that is tied -or tethered - to a fiat currency. USDT exists on several third-party blockchains, including Ethereum. USDT is a centralized stablecoin, which means the cryptocurrency is backed by U.S. Dollars and other assets held by Tether Limited. Tether Limited is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens. Tether seeks to peg USDT to the U.S. Dollar at a 1:1 ratio. (*Id.* at ¶ 17).

address had a pre-existing balance of approximately 732,738 USDT. (*Id.*) After the transfer, the subject cryptocurrency address had a balance of approximately 1,087,815 USDT. (*Id.*)

Between December 14, 2023 and December 21, 2023, approximately 139,921 USDT was transferred out of the subject cryptocurrency address. (*Id.* at ¶ 48(S).) On or about December 21, 2023, the USDT at the subject cryptocurrency address was frozen by Tether Limited. (*Id.* at ¶¶ 48(T), (U).) At the time of the freeze, the subject cryptocurrency address had a balance of approximately 947,883 USDT, including approximately $105,615.00 of the funds that originated in J.S.'s account. (*Id.*)

Pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jennifer D. Armstrong on July 31, 2024, 947,883 USDT tokens were transferred by Tether Limited to a U.S. law enforcement-controlled virtual currency wallet. (*Id.* at ¶ 7.)

B. Procedural History

On November 26, 2024, the United States filed its verified Complaint in Forfeiture in the total amount of 947,883 Tether Cryptocurrency (approximately $947,883.00). (Doc. No. 1.) Attached as Exhibits thereto are Notices of Forfeiture to the following three potential claimants: (1) cfo@c******.com; (2) m****ry*1@gmail.com; and (3) be*******.mer**@gmail.com. (Doc. Nos. 1-5, 1-6, and 1-7.) On that same date, the Clerk of Court issued a Warrant of Arrest *in Rem* (Doc. No. 2), which was executed on the Defendant Property by the United States Marshals Service on January 15, 2025.

Meanwhile, the United States posted notice of the Complaint in Forfeiture on an official government internet site, www.forfeiture.gov on November 26, 2024. (Doc. No. 9 at PageID#80; Doc. No. 9-2.) In relevant part, the notice provided as follows:

> Any person claiming a legal interest in the Defendant Property must file a verified Claim with the court within 60 days from the first day of publication (November 27, 2024) of this Notice on this official government internet web site and an Answer to the complaint or motion under Rule 12 of the Federal Rules of Civil Procedure within 21 days thereafter. 18 U.S.C. § 983(h)(1) permits a court to impose a civil fine on anyone asserting an interest in property which the court determines was frivolous.
>
> The verified Claim and Answer must be filed with the Clerk of the Court, Carl B. Stokes U.S. Courthouse, 801 West Superior Avenue, Cleveland, OH 44113, and copies of each served upon Assistant United States Attorney Asset Forfeiture Section, 400 U.S. Courthouse, 801 West Superior Avenue, Cleveland, OH 44113, or default and forfeiture will be ordered. See, 18 U.S.C. § 983(a)(4)(A) and Rule G(5) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions.

(Doc. No. 9-2 at PageID# 87.) The notice remained posted on the above website for at least thirty consecutive days, from November 27, 2024 to December 26, 2024. (Doc. No. 9 at PageID#80; Doc. No. 9-2 at PageID# 88.)

On December 5, 2024, the United States filed a notice on the docket indicating that, on November 27, 2024, it had served the Notices of Forfeiture, as well as copies of the verified Complaint, on each of the three potential claimants by electronic mail. (Doc. Nos. 3, 4, 5.) The United States further indicated that it did not receive "undeliverable" error messages showing either that the emails were not delivered or that the e-mail addresses were invalid. (*Id*.)

Pursuant to Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (hereinafter "the Supplemental Rules"), the potential claimants were required to file with the Court a verified claim to the Defendant Property within thirty (35) days after receipt of the Complaint. Here, the United States has filed a notice indicating that the three potential claimants herein received copies of the Complaint and Notice of Forfeiture via electronic mail on November 27, 2024, making their verified claims due by no later than January 2, 2025. A review of the docket demonstrates that, as of the date of this Order, no verified claims have been filed.

Accordingly, on February 4, 2025, the United States filed the instant Motion for a Final Order of Forfeiture. (Doc. No. 6.) The United States asserts that it has "satisfied all of the statutory notice requirements as set forth in Rule G(4) of the Supplemental Rules" and that "the only known potential third-party claimants to the defendant property have failed to file a verified claim to the defendant property … or an answer to the Complaint in Forfeiture." (*Id*. at p. 1.) The United States argues that, because $105,615.00 is traceable to J.S. and the fraud scheme, J.S. may be recognized as an "innocent owner" of that sum under 18 U.S.C. § 983(d)(2)(A) and, therefore, the United States Marshal should be directed to pay $105,615.00 directly to J.S. (*Id*. at p. 2.) The United States also argues that the remaining approximately $842,268.00 of the Defendant Property should be "finally forfeited to the United States under 18 U.S.C. § 981(a)(1)(A) (money laundering) and 18 U.S.C. § 981(a)(1)(C) (proceeds of wire fraud/conspiracy to commit wire fraud)." (*Id*.) *See also* Doc. No. 6-1 at PageID#s 47-51) (citing cases).

Finally, the United States argues that J.S. does not have an "ownership interest" in the remaining amount of his loss ($319,385.00) because the FBI was not able to trace any part of this amount to the subject cryptocurrency address. (Doc. No. 6 at p. 2.) The United States notes that, as an "alternative remedy," J.S. may "choose to submit a Petition for Remission or Mitigation to the U.S. Department of Justice, Criminal Division, seeking remission of the $319,385.00 from the forfeited property." (*Id*.) In this regard, the United States notes that "it is significant that J.S. is the only identified victim of the fraud scam [and], presumably, there will be no other/competing victim remission petitions." (*Id*. at pp. 2-3.)

On March 25, 2025, the Court issued an Order directing the United States to file a Supplement addressing certain issues. (Doc. No. 7.) The Court ordered the United States to (1) provide an

explanation as to who the three potential claimants are and the nature of the claims that they may have to the cryptocurrency at issue; (2) address whether it is appropriate for the potential claimants to be identified solely as email addresses; (3) explain the basis for its belief that service via email to the three potential claimants is reasonable under the circumstances; and (4) explain why J.S. is not considered a potential claimant in this action. (*Id*.) The United States submitted its Supplemental Brief on April 15, 2025. (Doc. No. 9.)

II. Analysis

A. Statutory Notice Requirements

The Court begins by evaluating whether the United States has satisfied the applicable statutory notice requirements. "The rules governing civil *in rem* forfeiture actions are found in 18 U.S.C. § 983 and Rule G of the" Supplemental Rules. *United States v. $31,000.00 in U.S. Currency*, 872 F.3d 342, 347 (6th Cir. 2017). "Rule G details various procedures with which parties to an *in rem* forfeiture action must comply." *Id*. Supplemental Rule G(4) requires the government to provide two forms of notice in a forfeiture action *in rem*: (1) notice to the public via publication, and (2) notice to potential claimants via direct notice. *See* Supp. R. G(4)(a), (b); *United States v. Twenty-Four Cryptocurrency Accounts*, 473 F.Supp.3d 1, 5 (D.D.C. 2020). For the reasons set forth below, the Court finds that the United States has satisfied the requirements set forth in Supplemental Rule G with respect to both forms of notice.

1. Notice by Publication

Pursuant to Supplemental Rule G(4)(a)(ii), notice by publication must describe the property that is the subject of the forfeiture with "reasonable particularity," state the time to file a claim and answer, and name the government attorney to be served with the claim and answer. *See* Supp. R.

G(4)(a)(ii). Such notice is sufficient if it is published "on an official internet government forfeiture site for at least 30 consecutive days." *Twenty-Four Cryptocurrency Accounts*, 473 F.Supp.3d at 5. *See also* Supp. Rules G(4)(a)(iii)(B) and 4(a)(iv)(C).

Here, the United States has presented evidence that it posted notice of the verified Complaint in Forfeiture herein on an official government internet site, www.forfeiture.gov, for 30 consecutive days, beginning on November 27, 2024 and ending on December 26, 2024. (Doc. No. 9-2.) As set forth *supra*, that notice properly set forth the time to file a verified claim and answer. (Doc. No. 9-2 at PageID# 87.) *See* Supp. R. G(5)(a)(ii)(B) and (5)(b). The notice also indicated that any claim and answer should be filed in this Court and served on "Assistant United States Attorney Asset Forfeiture Section." (Doc. No. 9-2 at PageID# 87.) Based on the above, the Court finds that the United States has fully satisfied the requirements for notice by publication set forth in Supp. R. G(4)(a). The United States indicates (and the docket reflects) that no claims were filed in response to the publication. (Doc. No. 6 at PageID#51.)

2. Direct Notice to Potential Claimants

The second form of notice is direct notice to potential claimants. Supplemental Rule G(4)(b) provides that direct notice must be sent "to any person who reasonably appears to be a potential claimant on the facts known to the government" and "by means reasonably calculated to reach the potential claimant." *Twenty-Four Cryptocurrency Accounts*, 473 F.Supp.3d at 5. *See* also Supp. R. G(4)(b)(i), (iii)(A); *Mesa Valderrama v. United States*, 417 F.3d 1189, 1197 (11th Cir. 2005) ("Reasonable notice ... requires only that the government attempt to provide actual notice; it does not require that the government demonstrate that it was successful in providing actual notice.") The direct notice must state: (1) the date when the notice is sent; (2) a deadline for filing a claim, at least

35 days after the notice is sent; (3) that an answer or a motion under Rule 12 must be filed no later than 21 days after filing the claim; and (4) the name of the government attorney to be served with the claim and answer. *See* Supp. R. G(4)(b)(ii). "Notice by the following means is sent on the date when it is placed in the mail, delivered to a commercial carrier, or sent by electronic mail." Supp. R. G(4)(b)(iv).

Here, the United States indicates that the "person[s]/entit[ies]" at the email addresses cfo@c******.com; m****ry*1@gmail.com; and be*******mer**@gmail.com are potential claimants in the instant case. (Doc. No. 6-1 at PageID#s 51-53.) On November 27, 2024, the United States emailed Notices of Forfeiture to these three email addresses, to which it attached copies of the verified Complaint in Forfeiture. (Doc. No. 1-5, 1-6, and 1-7.) Each of these Notices provides as follows:

> The above-captioned forfeiture action was filed in U.S. District Court on November 26, 2024. A copy of the Complaint in Forfeiture is attached. If you claim an interest in the defendant property, the following applies:
>
> Pursuant to Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, you are required to file with the Court, and serve upon James L. Morford, plaintiff's attorney, whose address is United States Attorney 's Office, 400 United States Court House, 801 West Superior Avenue, Cleveland, Ohio 44113, a verified claim to the defendant property within 35 days after your receipt of the complaint. The claim shall contain the information required by Rule G(5) of the said Supplemental Rules. Additionally, you must file and serve an answer to the complaint, or a motion under Rule 12 of the Federal Rules of Civil Procedure, within 20 days after the filing of the claim, exclusive of the date of filing. If you fail to do so, judgment will be taken for the relief demanded in the complaint.

(*Id*.) The United States indicates that "[t]he USAO did not receive an 'undeliverable' error message showing either that the e-mail[s] w[ere] not delivered or that the e-mail address[es] w[ere] invalid," and therefore the transmissions of the email messages to the three potential claimants were successful. (Doc. No. 6-1 at PageID#s 51-54.)

For the following reasons, the Court finds that the United States has satisfied the requirements set forth in Rule G for direct notice to potential claimants. First, the Court finds that the United States has sufficiently explained why it believes the three email addresses set forth above reasonably appear to represent potential claimants. In its Supplemental Brief, the United States asserts that, while traditional financial institutions (like a local bank) are required to keep, verify, and maintain Know-Your-Customer ("KYC") information about all customers (including names, birthdates, addresses, and telephone numbers), "the cryptocurrency space works in a substantially different manner." (Affidavit of FBI Special Agent Milan R. Kosanovich.[4] (Doc. No. 9-1) at PageID# 81-82.) Specifically, "[u]nlike the traditional financial system, a user in the cryptocurrency space does not need to involve any third party - such as a financial institution - to open an account." (*Id*. at PageID# 82.) Instead, "anyone using the applicable software can generate a wallet address for their cryptocurrency blockchain of choice without being required to provide any type of identifying information to anyone."[5] (*Id*.)

Here, however, the FBI was able to determine that the initial funds "invested" by J.S. were eventually converted to Tether ("USDT") cryptocurrency on the Ethereum blockchain. (*Id.* at PageID# 83.) As Agent Kosanovich explains:

> The Ethereum blockchain enables developers to build applications and tokens on the blockchain. Due to the frequently volatile nature of the cryptocurrency space, Tether

---

[4] Special Agent Kosanovich avers that he has been a Special Agent with the FBI since 2008. (Doc. No. 9-1 at PageID# 81.) He states that he has been "assigned to numerous criminal investigations involving complex financial crimes, complex computer crimes, and crimes facilitated through the Internet." (*Id*.) Agent Kosanovich avers that he is currently assigned to the FBI Cleveland Division Cyber Crimes Squad and is responsible for investigations involving computer-enabled offenses, including those involving cryptocurrency. (*Id*.)

[5] In his Affidavit, FBI Special Agent Kosanovich further explains that the only instance where KYC-type information would be maintained for a cryptocurrency user would be for a cryptocurrency account that is opened at a Virtual Currency Exchange ("VCE"). (Kosanovich Aff. at PageID# 82.) In the instant case, however, the subject cryptocurrency was not associated with a VCE. (*Id*. at PageID# 83.)

> Limited, Inc. ("Tether") developed a business plan to create a token on the Ethereum blockchain that would be backed by other assets to give the token a consistent value equal to one U.S. dollar. This plan required Tether to code a smart contract and deploy it on the Etheruem blockchain to create the token. This also resulted in Tether having the ability to freeze USDT in an address through specific adjustments in the relevant code. As in the instant case, Tether will freeze USDT in an address pursuant to lawful requests from law enforcement and judicial authorities. Upon such freeze, Tether does not control the cryptocurrency address itself but, rather, the USDT within that address. Tether can freeze any further transfers of USDT out of the specific address. In the instant case, the USDT at ADDRESS-7 was frozen by Tether on or about December 21, 2023. At the time of the freeze, ADDRESS-7 had a balance of approximately 947,883 USDT.
>
> Upon such freeze, an owner can review the Tether website to learn how the address owner can initiate contact with the company. Tether only accepts communications via an online form to be filled out on the "Contact Tether Support" portion of its website. When such an inquiry is made concerning a specific address, Tether will respond in two ways: (i) Tether will reply to the claimed owner with the contact information for the law enforcement entity that initiated the freeze; and, (ii) Tether will advise the law enforcement entity initiating the freeze as to information received from the claimed owner. As part of the e-mail communication between Tether and the claimed owner, there is no requirement that the claimed owner provide Tether with any kind of verified KYC-type identifying information. The only certain piece of information that Tether will provide to the law enforcement entity is the e-mail address used by the claimed owner to make the inquiry.
>
> In the instant case - concerning the freeze of the subject cryptocurrency address beginning/ending 0x7d5 ... 48a8306 (ADDRESS-7) - Tether received inquiries from three different e-mail addresses; namely, the e-mail addresses: [cfo@c******.com; m****ry*1@gmail.com; and be*******mer**@gmail.com].

(*Id*. at PageID#s 83-84.)

The United States contends that it reasonably concluded that the three email addresses that submitted inquiries to Tether represented "potential claimants" for purposes of Supplemental Rule G. The Court agrees. While the viability of any of these three inquiries could not be fully assessed unless and until a claim and answer was filed (which did not occur here), the Court agrees that it was

reasonable, under the circumstances, for the United States to presume that the senders of inquiries regarding the frozen cryptocurrency at issue here constituted "potential claimants." [6]

The Court further finds that the United States' use of email notification to provide direct notice was "reasonably calculated to reach the potential claimant." *Twenty-Four Cryptocurrency Accounts*, 473 F.Supp.3d at 5. Federal courts have found that, under certain circumstances, direct notice to potential claimants may be made via email under Supplemental Rule G(4). *Id.* at 6 (noting that "email was an appropriate form of notice under these circumstances because the case involves international defendants whose locations are hard to pin down and the nature of the crimes necessarily entails some degree of cyber-proficiency on the part of the Defendant Properties' owners."). *See also United States v. 155 Virtual Currency Assets*, 2021 WL 1340971 at * 5 (D.D.C. April 9, 2021) (same); Supp. R. G(4)(b)(iv).

Here, due to the inherently anonymous nature of the "cryptocurrency space," the three email addresses noted above were the only identifying and/or contact information available to the United States regarding the potential claimants. Moreover, given that the potential claimants themselves used the email addresses noted above to contact Tether concerning the freeze of the cryptocurrency, the Court finds that it was reasonable for the United States to send direct notice to the potential claimants at those email addresses. And, as the United States correctly notes, the United States' email notifications to cfo@c******.com; m****ry*1@gmail.com; and be*******mer**@gmail.com

[6] The Court also agrees with the United States that "while a claimed owner of the defendant property might have felt comfortable reaching out to a private company (i.e., Tether Limited Inc.), it might not have been willing to make itself known and identifiable to the Court and public through a formal response to the Complaint in Forfeiture." (Kosanovich Aff. at PageID#s 84-85.)

were not returned as undeliverable. Accordingly, the Court finds that the United States' use of email notification to provide direct notice to the potential claimants here satisfied Supplemental Rule G.

Finally, the Court finds that the content of the Notices of Forfeiture sent to cfo@c******.com; m****ry*1@gmail.com; and be*******mer**@gmail.com satisfied Supplemental Rule G(4)(b)(ii). Specifically, each of the Notices (Doc. Nos. 1-5, 1-6, and 1-7) provided (1) the date when the notice was sent; (2) a deadline for filing a claim, at least 35 days after the notice is sent; (3) notice that an answer or a motion under Rule 12 must be filed no later than 21 days after filing the claim; and (4) the name of the government attorney to be served with the claim and answer. *See* Supp. R. G(4)(b)(ii).

Accordingly, the Court finds that the United States has satisfied the requirements for direct notice set forth in Supp. R. G(4)(b). As noted *supra,* the docket reflects that none of the potential claimants filed verified claims and/or answers in the instant action.

B. Forfeitability

The Complaint in Forfeiture seeks forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C), alleging that the Defendant Property was (1) involved in money laundering in violation of 18 U.S.C. § 1956 (money laundering); and (2) traceable to an offense which constitutes "specified unlawful activity" ("SUA"), i.e., wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud offenses in violation of 18 U.S.C. § 371. The Court will address each of these bases for forfeiture separately, below.

1. Money Laundering

In the Complaint, the United States alleges that "[t]he transfer of the 355,077 USDT on December 14, 2023, from ADDRESS-6 into ADDRESS-7 … constituted a transaction in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering)." (Doc. No. 1 at ¶ 50.) The

United States further alleges that "[a]t the time of the transfer, ADDDRESS-7 had a pre-existing balance of 732,738 USDT." (*Id*.) The United States then alleges as follows:

> Under 18 U.S.C. Section 981(a)(l)(A), the entire defendant property - namely, 947,883 USDT ($947,883.00) - is forfeitable. The "other funds" that were commingled with the 105,615 USDT belonging to J.S. in the December 14, 2023, transfer of approximately 355,077 USDT from ADDRESS-6 to ADDRESS-7 - and the pre-existing balance of approximately 732,738 USDT in ADDRESS-7 - also were "involved in" the concealment money laundering offense and, accordingly, are subject to forfeiture in that they facilitated the violation by helping to conceal the nature, source, ownership, and/or control of the USDT traceable to J.S.

(*Id*. at ¶ 52.) In its Motion for Final Order of Forfeiture, the United States reasserts that the "other funds" that were commingled with J.S.'s funds are forfeitable because the "other funds" facilitated a money laundering transaction. (Doc. No. 6-1 at PageID#s 48-49.) The United States cites numerous decisions in support of its argument, including decisions from the First, Fifth, Sixth, Eighth, and D.C. Circuit Courts of Appeals. (*Id*.) (citing cases).

The Court agrees with the United States. Title 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct "a financial transaction which in fact involves the proceeds of specified unlawful activity . . . knowing that the transaction is designed in whole or in part - to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity." 18 U.S.C § 1956(a)(1)(B)(i). Section 981(a)(1)(A) of Title 18 provides that:

> (a)(1) The following property is subject to forfeiture to the United States:
>
> (A) Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property.

18 U.S.C. § 981(a)(1)(A). Interpreting these statutes, the Sixth Circuit has found that, under certain circumstances, the commingling of fraud proceeds with untainted money as part of concealment

money laundering under § 1956(a)(1)(B)(i) permits the forfeiture of the untainted money. *United States v. Coffman*, 574 Fed. Appx. 541, 561 (6th Cir. 2014). Specifically, the Sixth Circuit explained:

> Under the forfeiture statute, "property" that is "involved in" an offense "or any property traceable to such property" is forfeitable. 18 U.S.C. § 982(a)(1). "Property under the statute includes the money or other property being laundered (the corpus), any commissions or fees paid to the launderer, and any property used to facilitate the laundering offense." *United States v. Puche*, 350 F.3d 1137, 1153 (11th Cir. 2003) (internal citations and quotation marks omitted). "Facilitation occurs when the property makes the prohibited conduct less difficult or more or less free from obstruction or hindrance." *Id*.
>
> Commingling of fraud proceeds with untainted money as part of concealment money laundering under 18 U.S.C. § 1956(a)(1)(B)(i) permits the forfeiting of the untainted money in certain circumstances. *Puche*, 350 F.3d at 1153. "Forfeiture of commingled funds ... is proper when the government demonstrates that the defendant pooled the funds to facilitate or disguise his illegal scheme." *Id*. Commingling "is enough to expose the legitimate funds to forfeiture, if the commingling was done for the purpose of concealing the nature or source of the tainted funds (that is, if the commingling was done to facilitate money laundering in violation of 18 U.S.C. § 1956(a)(1)(B)(i))." *United States v. McGauley*, 279 F.3d 62, 76 (1st Cir. 2002).

Id.[7] As the United States correctly notes, several other Circuit Courts of Appeals and district courts have reached the same conclusion. *See, e.g., United States v. McGauley*, 279 F.3d 62, 69 (1st Cir. 2002) (affirming district court's jury instruction that "forfeiture of legitimate and illegitimate funds commingled in an account is proper as long as the Government demonstrates to you … that the defendant pooled the funds, comingled the funds, moved the funds to facilitate – that is, to disguise the nature or source or the location of the funds"); *United States v. Bornfield*, 145 F.3d 1123, 1125

---

[7] While 18 U.S.C. § 982(a)(1) involves criminal forfeiture, the "involved in" and "traceable to" language in that section is identical to that contained in 18 U.S.C. § 981(a)(1), which governs civil forfeitures. *Compare* § 982(a)(1) ("The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.") with § 981(a)(1)(" The following property is subject to forfeiture to the United States: (A) Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property.") *See McGauley*, 279 F.3d at fn 13 (noting that "the terms 'involved in' and 'traceable' are also found in the civil forfeiture provision, 18 U.S.C. § 981(a)(1)" and stating that "we look to cases under both § 981 and § 982 for guidance in interpreting these terms.")

(10th Cir. 1998) (finding that "forfeiture of legitimate and illegitimate funds commingled in an account is proper as long as the government demonstrates that the defendant pooled the funds to facilitate, i.e., disguise the nature and source of, his scheme"); *United States v. Cessa*, 872 F.3d 267, 273-274 (5th Cir. 2017) ("Property 'involved in' an offense 'includes the money or other property being laundered (the corpus), any commissions or fees paid to the launderer, and *any property used to facilitate the laundering offense*.'") (quoting *United States v. Tencer*, 107 F.3d 1120, 1134 (5th Cir. 1997)) (emphasis in original). *See also United States v. Real Property located at 6415 Harrison Avenue, Fresno, California*, 2011 WL 2580335 at * 4 (E.D. Cal. June 28, 2011) ("Although section 981(a)(1)(A) does not contain the words 'facilitate' or 'facilitating,' numerous courts have concluded that the phrase 'property involved in' includes property used to facilitate an offense.") (collecting cases).

Here, the Court finds that the United States has sufficiently demonstrated that the entirety of the Defendant Property is subject to forfeiture under § 981(a)(1)(A). The FBI conducted a detailed tracing analysis of J.S.'s stolen funds. (Doc. No. 1 at ¶ 47-48.) As set forth in Paragraph 48 of the verified Complaint, the FBI determined through its investigation that, during the roughly two month period between October 19, 2023 and December 24, 2023, the fraudsters repeatedly transferred some or all of J.S.'s funds to different addresses, often "swapping" cryptocurrencies in the process. (*Id*. at ¶ 48.) The United States alleges that the execution of some of these transactions resulted in significant costs, solely to obtain a different version of cryptocurrency. (*Id.* at ¶ 48(B)). The United States also alleges that "[m]oving cryptocurrency from one stablecoin (USDT) to another (DAI) and back again in a short time would be an extremely unusual investment strategy as both USDT and DAI strive to reflect a value on par with a 1:1 ratio with the U.S. Dollar and, therefore, have only minor fluctuations

in value." (*Id.* at ¶ 48(N)). The United States alleges that "[g]iven the fees and costs incurred for each transaction, it is unlikely that this strategy would ever profit an investor" and, therefore, "the most likely reason for these transaction was to engage in concealment money laundering of stolen funds." (*Id*.)

As the Sixth Circuit has noted "'[w]hen a sequence of transactions is sufficiently complex, a reasonable juror may infer that the transactions were made for the purpose of concealment.'" *Coffman*, 574 Fed. Appx. at 561 (quoting *United States v. Warshak*, 631 F.3d 266, 321 (6th Cir. 2010)). Here, the Court finds that the United States has sufficiently demonstrated that the transactions involving J.S.'s stolen funds were made for the purpose of concealment. Specifically, and based on the detailed (and uncontested) allegations in the verified Complaint, the Court concludes that J.S's funds were commingled with the funds that were transferred to ADDRESS-7 (in the total amount of 947,883 USDT ($947,883.00)) and, further, that these "other funds" were "involved in" the concealment money laundering violation because they facilitated the violation by helping to conceal the nature, source, ownership, and/or control of the USDT traceable to J.S.

Accordingly, the Court concludes that the entire Defendant Property is subject to forfeiture under § 981(a)(1)(A).

2. Wire Fraud

In the verified Complaint, the United States further alleges that:

> The entire defendant property - namely, 947,883 USDT ($947,883.00) - also is subject to forfeiture under 18 U.S.C. Section 98l(a)(l)(C) as property which constitutes, or is derived from, proceeds traceable to an offense(s) constituting "specified unlawful activity" - as defined in 18 U.S.C. Section 1956(c)(7), with reference to 18 U.S.C. Section 1961(1) - namely: wire fraud, in violation of 18 U.S.C. Section 1343, and conspiracy to commit wire fraud, in violation of 18 U.S.C. Section 371. In addition to the funds stolen from J.S., the other USDT funds seized from ADDRESS-7 appear

> to be the proceeds of fraud in that they bear the hallmarks of similar money laundering activity - with no economic purpose - before being deposited into ADDRESS-7.

(Doc. No. 1 at ¶ 53.) In its Motion, the United States also seeks an order finding that the entire Defendant Property is subject to forfeiture under § 981(a)(1)(C). (Doc. No. 6-1 at PageID#s 50-51.)

The Court agrees with the United States. Title 18 U.S.C. § 1343 makes it a crime for anyone, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice. *See* 18 U.S.C. § 1343.

Section 981(a)(1)(C) of Title 18 authorizes the forfeiture of any property "which constitutes or is derived from proceeds traceable to ... any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense." 18 U.S.C. 981(a)(1)(C). *See also United States v. Coffman*, 612 Fed. Appx. 278, 282 (6th Cir. 2015). Wire fraud is a "specified unlawful activity." *See* 18 U.S.C. § 1956(c)(7)(A) (designating as a "specified unlawful activity" any act constituting an offense "listed in section 1961(1) of this title"); *id.* § 1961(1) (listing wire fraud). *See also Coffman*, 612 Fed. Appx. at 282. Thus, any proceeds of the fraud are forfeitable. *Coffman*, 612 Fed. Appx. at 282.

Based on the uncontested allegations in the verified Complaint, the Court agrees that, in addition to the funds stolen from J.S., the other USDT funds seized from ADDRESS-7 appear to be the proceeds of fraud because they bear the hallmarks of similar money laundering activity before being deposited into ADDRESS-7. Accordingly, the Court concludes that the entire Defendant Property is also subject to forfeiture under § 981(a)(1)(C).

C. Innocent Owner

Lastly, the United States asks that the Court recognize J.S. as an "innocent owner" of $105,615.00 of the forfeited funds, and order the Marshals Service to pay that sum directly to J.S. (Doc. No. 6 at PageID# 40.) In support of this request, the United States asserts as follows. J.S. is the only victim of the cryptocurrency fraud scam who has been particularly identified by the FBI. (*Id.*) Through several steps of blockchain analysis, FBI investigators were able to trace approximately $105,615.00 of J.S.'s funds to the subject cryptocurrency address. (*Id.*) Because the $105,615.00 is traceable to J.S. and the fraud scheme, the United States argues that J.S. may be recognized as an "innocent owner" of the $105,615.00 under 18 U.S.C. § 983(d)(2)(A). (*Id.*)

Thus, the United States requests that this Court order that (1) $105,615.00 of the Defendant Property be paid by the Marshals Service to J.S; and (2) the remaining approximately $842,268.00 of the defendant property be finally forfeited to the United States under 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). (*Id.*) With respect to the remaining loss ($319,385.00) incurred by J.S., the United States maintains that the FBI was not able to trace any part of this amount to the subject cryptocurrency address. (*Id.*) Accordingly, the United States argues that, under 18 U.S.C. § 983(d)(6), J.S. does not have an "ownership interest" in the Defendant Property beyond the $105,615.00 to be returned to him by the USMS and may not be viewed as an innocent owner as to any part of the $319,385.00. (*Id.*) However, as an alternative remedy, the United States asks that the Court's Final Order provide that J.S. may choose to submit a Petition for Remission or Mitigation to the U.S. Department of Justice, Criminal Division, seeking remission of the $319,385.00 from the forfeited property. (*Id.*)

In its Supplemental Briefing Order, the Court noted that "it would be helpful to this Court to understand why J.S. is not considered a potential claimant in this action." (Doc. No. 7.) The Court explained that it sought to ensure that J.S. had been provided sufficient opportunity to submit a claim or otherwise to argue, in this Court, that he is entitled to additional proceeds beyond the $105,615.00 that the United States submits he should be paid. (*Id.*) The Court asked the United States to be sure to address the Court's concerns regarding J.S. in its Supplemental Brief. (*Id.*)

As requested, the United States provided a thorough explanation of (1) why it decided to recognize J.S. as an "innocent owner" as to the $105,615.00 that the FBI was able to trace to J.S. and the fraud scheme; and (2) the reasons that J.S. cannot be considered a potential claimant under Supplemental Rule G(4)(b)(i). (Doc. No. 9 at PageID#s 74-79.) The United States also provided additional detail and explanation regarding the Petition for Remission or Mitigation remedy that is available to J.S. with regard to his remaining loss ($319,385.00). The Court appreciates the United States' attention to the Court's concerns, and is satisfied by the United States' response.

III. Conclusion

Accordingly, and for all the reasons set forth above, the United States' Motion for Forfeiture (Doc. No. 6) is GRANTED. The Court hereby ORDERS as follows:

1. The Defendant Property in the instant case is 947,883 Tether ("USDT") cryptocurrency, valued at approximately $947,883.00, and formerly associated with the cryptocurrency address beginning/ending 0x7d5 . . . 48a8306.

2. Based upon the foregoing, and under 18 U.S.C. § 983(d)(2)(A), J.S. has an innocent owner interest in the defendant property to the extent of $105,615.00.

3. $105,615.00 of the defendant property shall be paid by the United States Marshals Service ("USMS") to J.S. The FBI shall provide the identifying and contact information for J.S. to the USMS.

4. The remaining approximately $842,268.00 of the defendant property is finally forfeited to the United States under 18 U.S.C. § 981(a)(1)(A) (money laundering) and 18 U.S.C. § 981(a)(1)(C) (proceeds of wire fraud/conspiracy to commit wire fraud), and no right, title, or interest shall exist in any other party. The United States shall seize and take control of the approximately $842,268.00 and shall dispose of it in accordance with law.

5. As set forth above, J.S. - a senior citizen - lost his entire life savings as a result of the cryptocurrency fraud scam. In total, J.S. lost approximately $425,000.00. Of this amount - as ordered above - $105,615.00 of the Defendant Property shall be returned to J.S. by the USMS. With respect to the remaining loss amount ($319,385.00), which the FBI was not able to trace to the subject cryptocurrency address, J.S. may choose to submit a Petition for Remission or Mitigation to the U.S. Department of Justice, Criminal Division, seeking remission of the $319,385.00 from the forfeited property. As set forth above, J.S. is the only victim of the cryptocurrency fraud scam who has been identified by the FBI.

IT IS SO ORDERED.

s/Pamela A. Barker
PAMELA A. BARKER
U. S. DISTRICT JUDGE

Date: April 24, 2025